

KENT S. ROBINSON  
Acting United States Attorney  
District of Oregon  
CHRISTOPHER L. CARDANI  
Assistant United States Attorney  
405 East Eighth Avenue, Suite 2400  
Eugene, Oregon 97401  
(541) 465-6771  
[chris.cardani@usdoj.gov](mailto:chris.cardani@usdoj.gov)  
CHARLES F. GORDER, JR., OSB# 912874  
Assistant United States Attorney  
1000 SW Third Avenue, Suite 600  
Portland, Oregon 97204  
(503) 727-1117  
[charles.gorder@usdoj.gov](mailto:charles.gorder@usdoj.gov)

IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF OREGON

UNITED STATES OF AMERICA,	)	
	)	
Plaintiff,	)	Case No. 05-CR-60008-HO
	)	
v.	)	
	)	
PIROUZ SEDAGHATY,	)	GOVERNMENT'S RESPONSE
	)	TO DEFENDANT'S SUPPLEMENT TO
	)	MOTION TO SUPPRESS
Defendant.	)	

**I. Introduction**

The United States of America, through its undersigned counsel, herein responds to Defendant's Supplement to Motion to Suppress (CR 213). Through his supplement, defendant again seeks to have the Court suppress all the fruits of searches of computers seized by the government pursuant to Judge Cooney's search warrant. The supplemental motion relies on the recent *en banc* decision of the Ninth Circuit in *United States v. Comprehensive Drug Testing, Inc.*, 579 F.3d 989, 2009 WL 2605378 (9th Cir.

August 26, 2009) (“CDT”). For reasons set forth below, this Court should rule that *CDT* does not compel suppression.

## **II. Factual Background**

A detailed factual background of the search warrant and execution procedures is set forth in the government’s response to defendant’s motion to suppress (CR 192), which should be examined along with this response. That factual summary was supplemented by the testimony of Special Agent Anderson at the July 13, 2009 suppression hearing. From the response and testimony, this Court learned in some detail the procedures used by the government in seeking the search warrant, the terms of the warrant, and the conduct of the government in executing the warrant and reviewing information within the seized computers.

After the suppression hearing the government filed a tentative exhibit list with the Court, as required. This list identifies numerous exhibits the government will rely on at trial that were derived from the computer searches challenged by defendant’s motion.

## **III. Argument**

### **A. Comprehensive Drug Testing, Inc. Does Not Apply Retroactively**

The facts in *CDT* are highly unusual in that they involved a subpoena and search warrant served on a third party, uninvolved in criminal activity, for electronic records concerning drug test results for professional baseball players. The appeal did not involve a motion to suppress, requiring a traditional Fourth Amendment analysis. Rather, the aggrieved parties had filed motions before the district court under Fed. R. Crim. P. 17(c) and 41(g) seeking to have the subpoena quashed and their seized

property returned. As explained below, this distinction is important in this case.

The Ninth Circuit used the opportunity in *CDT* to create a set of unprecedented procedures to be used in writing search warrants and subsequently searching the contents of electronic evidence. These new procedures dramatically alter the manner in which the government will be able to obtain future warrants and search electronically stored information seized under those warrants.

Perhaps recognizing the impact of its decision, the majority in *CDT* appears to emphasize that it intends that its new procedures will apply only to *future* computer search warrants. *CDT*, 2009 WL 2605378, at \*7 (“ . . . the government should, in future warrant applications, forswear reliance on the plain view doctrine . . . .”); *id.* (“ . . . lack of candor . . . shall bear heavily against the government in the calculus of any subsequent motion . . . .”); *id.* at \*9 (“To guard against such unlawful conduct in the future, the warrant application should normally include . . . a protocol for preventing agents . . . from examining or retaining any data other than that for which probable cause is shown.”). Thus, by its own language, the Ninth Circuit does not intend its *CDT* opinion to be applied retroactively.

Not holding the government to strict conformance to the new *CDT* rules in past computer search warrants and past computer searches is especially appropriate in light of the fact that the opinion *sub silentio* reverses previous numerous Ninth Circuit decisions regarding computer searches.<sup>1</sup> If *CDT* were deemed to apply retroactively, all

---

<sup>1</sup>In pages 24 and 28-32 of its response to defendant’s motion to suppress (CR 192), the government reviewed a series of relatively recent Ninth Circuit cases on computer search warrants and searches of seized computers which were governing in

computer search cases in this Circuit which are currently under investigation or prosecution would most likely face suppression of critical evidence, even if investigators and prosecutors were faithfully following then controlling Ninth Circuit law. It appears that the Ninth Circuit desired to avoid this result when, in three instances, it used language indicating that its new rules would only apply to cases involving computer searches which occurred after the issuance of the *CDT* opinion on August 26, 2009.

This sentiment is consistent with cases such as *Halliday v. United States*, 394 U.S. 831, 833 (1969). In *Halliday*, the Supreme Court considered whether a prior decision, *McCarthy v. United States*, 394 U.S. 459 (1969) - holding that defendants who pleaded guilty without strict adherence to procedures in Fed. R. Crim. P. 11 had to be given the opportunity to plead anew - was to be applied retroactively. The *Halliday* Court ruled that it did not. In concluding that its new decision was not to be applied retroactively, the Court was sensitive to the number of prior guilty pleas which may be impacted by the decision even though they were otherwise made in a voluntary manner. The Court wrote, "... in view of the large number of constitutionally valid convictions that may have been obtained without full compliance with Rule 11, we decline to apply *McCarthy* retroactively." *Id.* at 833; *see also United States v. McWilliams*, 730 F.2d 1218, 1223-24 (9<sup>th</sup> Cir. 1984) (recognizing *McCarthy* applied only prospectively and that the validity of prior guilty pleas was to be examined by "then governing standards of proof.").

---

this Circuit prior to the *CDT* decision.

It is significant that in all of its computer search decisions issued during the last decade, the Ninth Circuit refused to impose the type of rigid requirements now mandated by *CDT*. For instance, at the time our warrant was obtained in 2004, *United States v. Hay*, 231 F.3d 630 (9<sup>th</sup> Cir. 2000) was the most recent computer search decision in the Ninth Circuit. *Hay* interpreted *United States v. Tamura*, 694 F.2d 591 (9<sup>th</sup> Cir. 1982), which was relied heavily upon by the majority in *CDT*. In *Hay*, the Ninth Circuit held that *Tamura* did not apply to a scenario where the government had justified to the magistrate why it was necessary for wholesale seizure and off-site review of computer evidence, and the magistrate had given authorization to do so in the search warrant. 231 F.3d at 637. The Ninth Circuit rejected the defendant's argument that *Tamura* required the magistrate to "approve seizure of materials beyond those described in the warrant before wholesale removal occurs." *Id.*

In 2006, while the government was continuing to analyze the computers seized from defendant Sedaghaty in this case, the Ninth Circuit decided *United States v. Hill*, 459 F.3d 966 (9<sup>th</sup> Cir. 2006). *Hill* specifically stated that wholesale removal of computers by the government and subsequent review is appropriate where the government's affidavit in support of the warrant demonstrates why such broad authority is necessary to "seize the haystack to look for the needle." *Id.* at 975 (holding search warrant overbroad for its failure to include an explanatory supporting affidavit). Further, the *Hill* decision found no error where the government did not utilize a search protocol for reviewing the seized computers. *Id.* at 977. The court simply reiterated the "longstanding principle" that the government can never use a warrant to engage in a

general explanatory search and that the reasonableness of the government's search of seized materials is subject to judicial review. *Id.* at 978.

The holdings of both *Hay* and *Hill* are important because they demonstrate that, prior to the *CDT* decision, the Ninth Circuit had not mandated and, in fact, had rejected, the creation of specific procedures limiting computer searches beyond those which a well informed magistrate would approve. There was no prior indication that the government should waive the plain view doctrine, employ taint teams, or return to the magistrate to expand search protocols. It is thus appropriate, as the *CDT* decision indicates, that the radically new procedures identified in *CDT* be deemed to not have retroactive application.

*United States v. Gonzalez* Does Not Command a Different Result on the Retroactivity Question

In *United States v. Gonzalez*, No. 07-30098, 2009 WL 2581738 (9<sup>th</sup> Cir. August 24, 2009), the Ninth Circuit recently grappled with the question of when a Supreme Court decision construing the Fourth Amendment is to be applied retroactively. In *Gonzalez*, the Ninth Circuit concluded that a Supreme Court decision interpreting the Fourth Amendment, *Arizona v. Gant*, 129 S. Ct. 1710 (2009), must be applied retroactively based on the “long-standing precedent governing the applicability of a new rule announced by the Supreme Court while a case is on direct review.” *Id.* at \*2; see also *United States v. Johnson*, 457 U.S. 537, 562 (“[A] decision of this Court construing the Fourth Amendment is to be applied retroactively to all convictions that were not yet final at the time the decision was rendered.”); *Griffith v. Kentucky*, 479 U.S. 314, 328

(1987).

In arriving at this conclusion on retroactivity, the Ninth Circuit appears to have found significant the fact that the new decision under consideration was a Supreme Court opinion interpreting the Constitution. *Gonzalez* at \*2-3. The *CDT* opinion is not such a case. The Ninth Circuit opinion creates broad new procedures for computer search warrants and does not appear to be based on an interpretation of the Fourth Amendment. Rather, the decision is premised upon an application of Fed. R. Crim. P. 41 and the rebirth of principles articulated by the Ninth Circuit two and a half decades ago in *United States v. Tamura*, 694 F.2d 591 (9<sup>th</sup> Cir. 1982) (a case which did not involve a computer search), extended in *CDT* to evolving technology.<sup>2</sup> Once again, *CDT* should not be applied retroactively.

#### **B. Even if CDT Applies Retroactively, the Exclusionary Rule Does Not Apply**

If an officer executes a warrant while reasonably believing it to be valid, then the exclusionary rule does not apply. *United States v. Meek*, 366 F.3d 705, 714 (9<sup>th</sup> Cir. 2004); see also *Herring v. United States*, 129 S. Ct. 695, 701 (2009); *Hudson v. Michigan*, 126 S.Ct. 2159, 2163 (2006) (“Suppression of evidence . . . has always been our last resort.”); *United States v. Leon*, 468 U.S. 897, 906 (1984). When invoking the good faith exception, the government must prove that the officers relied on the warrant “in an objectively reasonable manner.” *United States v. SDI Future Health, Inc.*, 568

---

<sup>2</sup>It is worth noting that two dissenting opinions in *CDT* identify the new computer search procedures in the majority opinion as *dicta*. *CDT*, 2009 WL 2605378, at \*21 (Callahan, C.J., Ikuta, C.J., concurring in part and dissenting in part); *id.* at \*26 (Bea, C.J., concurring in part and dissenting in part).

F.3d 684, 706 (9<sup>th</sup> Cir. 2009). Where officers are “motivated by considerations of practicality rather than by a desire to engage in indiscriminate fishing” the Ninth Circuit has held that the fruits of an otherwise valid warrant need not be suppressed. *Hill*, 459 F.3d at 977 (holding that evidence of child pornography should not be suppressed where officers failed to justify the wholesale seizure of defendant’s zip disks in affidavit for search warrant to locate images). The good faith exception is not available if an officer should have known a rule was unconstitutional and still followed that rule. *Meek*, 366 F.3d at 714. In *Meek*, the officers were found to have acted in good faith because there “was no analogous precedent that could arguably have put an officer on notice that the statute” in question could be unconstitutional. *Id.* In fact, the statute had previously been held constitutional by the California Courts of Appeal. *Id.*

As reviewed above, the state of Ninth Circuit law for computer searches at the time of our search in 2004 was clear based on *Hay* and *Hill*. See discussion, *supra*. More recently, the Ninth Circuit again held that the standard for a computer search is reasonableness and that a heightened Fourth Amendment standard for computer searches was not necessary. *United States v. Giberson*, 527 F.3d 882, 888-89 (9<sup>th</sup> Cir. 2008) (“[T]he potential intermingling of materials does not justify an exception or heightened procedural protections for computers beyond the Fourth Amendment’s reasonableness requirement.”).

As measured by then existing law, the government’s actions were eminently and objectively reasonable. Obtaining a warrant to seize defendant Sedaghaty’s computers, and the subsequent search of the contents of those computers, were done



in good faith and in a manner consistent with controlling law at the time. The agent's good faith and respect for defendant's constitutional rights in this case is demonstrated in many ways. Special Agent Anderson prepared a detailed affidavit in support of the government's warrant request, properly incorporated the affidavit into the search warrant, and agents have relied on that affidavit in searching the seized computers.<sup>3</sup>

The Court knows from the suppression hearing that Special Agent Anderson was in close consultation with the Assistant United States Attorney in drafting the application for the warrant, establishing and following search procedures before and during the search, and in subsequently searching the contents of the seized computers. All law enforcement involved in the initial search were required to read the warrant affidavit and searching agents have continued to rely on the affidavit without any reason to believe that the search procedures were unreasonable.<sup>4</sup> Procedures were implemented to minimize the possibility of reading communications potentially covered by the attorney-client privilege. When suspected child pornography was discovered in defendant Sedaghaty's computers, another search warrant was obtained. In limiting the review of the contents of the computers, agents used search terms reasonably related to the investigation, rather than engaging in a wholesale, indiscriminate rummaging of the contents of the computers. These procedures reflect reasonableness at every stage.

---

<sup>3</sup>Attachment B to the Search Warrant states that "computer personnel may examine all of the data contained in the computer equipment and storage devices to view their precise contents and determine whether the data falls within the items to be seized as set forth herein."

<sup>4</sup>It should be noted that, based on *CDT*, the prosecutors ordered agents to cease further examination of the seized hard drives until further notice.

When an officer consults with a government attorney prior to submitting her affidavit to a magistrate judge, that consultation “is of significant importance to a finding of good faith.” *United States v. Brown*, 951 F.2d 999, 1005 (9th Cir. 1991); see also *United States v. Mendonsa*, 989 F.2d 366, 369-70 (9th Cir. 1993) (applying good faith exception where officer relied upon advice of attorney that his affidavit was complete). After consulting with an attorney and a neutral and detached magistrate, “the officers were not required to disbelieve these experts.” *Brown*, 951 F.2d at 1005, citing *Massachusetts v. Sheppard*, 468 U.S. 981, 989-990 (1984).

As stated earlier this year by the Supreme Court, the exclusionary rule only applies where police need to be deterred from deliberately violating the constitutional rights of an accused. *Herring*, 129 S. Ct. at 700-01. *The Gonzalez* decision, discussed above, does not command a different result. While the *Gonzalez* court refused to recognize the good faith exception, and distinguished *Herring*, the situation was different than our case. The Ninth Circuit found the Supreme Court’s *Herring* good faith analysis inapplicable because, unlike *Herring*, *Gonzalez* involved the applicability of a Supreme Court case interpreting the Fourth Amendment. As stated above, the present case does not involve a Fourth Amendment analysis; it is a rule based decision. Also, as discussed above, *CDT* is not retroactive.

In sum, the search and seizure methodology described above, including close coordination with the prosecutor, reflects actions taken with a respect for the law and defendant’s rights. Engaging in these prudent activities, and complying with computer search principles blessed by the Ninth Circuit at the time of the seizure and subsequent

search of defendant's computers, warrant application of the good faith exception should this Court find any violations of applicable search warrant law.

**IV. Conclusion**

*CDT* is not retroactive. Regardless, agents acted in good faith reliance on the search warrant in seizing and examining defendant's computers. This Court should deny defendant's motion to suppress the computer related evidence.

DATED this 9th day of October, 2009.

Respectfully submitted,

KENT S. ROBINSON  
Acting United States Attorney  
District of Oregon

*/s/ Christopher L. Cardani*

By: \_\_\_\_\_  
CHRISTOPHER L. CARDANI  
Assistant United States Attorney

*/s/ Charles F. Gorder, Jr.*

By: \_\_\_\_\_  
CHARLES F. GORDER, JR.  
Assistant United States Attorney